[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/08 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200580030718.4

[43] 公开日 2007 年 8 月 15 日

[11] 公开号 CN 101019369A

[22] 申请日 2005.7.8
[21] 申请号 200580030718.4
[30] 优先权
[32] 2004. 7.14 [33] US [31] 10/892,256
[86] 国际申请 PCT/US2005/024374 2005.7.8
[87] 国际公布 WO2006/023151 英 2006.3.2
[85] 进入国家阶段日期 2007.3.13
[71] 申请人 英特尔公司
地址 美国加利福尼亚州
[72] 发明人 J·苏顿二世 E·布里克尔
C·哈尔 D·格劳罗克
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 李亚非 梁 永

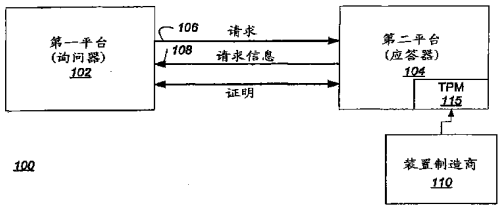
权利要求书 5 页 说明书 16 页 附图 12 页

[54] 发明名称

利用在线服务向装置传递直接证明私有密钥的方法

[57] 摘要

向安装在客户端计算机系统中的现场的装置传递直接证明私有密钥可以以安全的方式来完成，而不需要该装置中相当大的非易失性存储器。 在制造时生成唯一的伪随机值并将其存储在该装置中。 该伪随机值被用来生成用于加密数据结构的对称密钥，该数据结构保存直接证明私有密钥和与该装置相关的私有密钥摘要。 在客户端计算机系统可访问的受保护在线服务器上存储所得到的加密的数据结构。 当在客户端计算机系统上初始化该装置时，该系统检查在该系统中是否存在本地化的加密的数据结构。 如果不存在，该系统就利用安全协议从受保护在线服务器获得相关的加密的数据结构。 该装置利用从其存储的伪随机值再生的对称密钥对该加密的数据结构进行解密，以获得直接证明私有密钥。如果该私有密钥是有效的，它就可以用于客户端计算机系统中该装置随后的验证处理。



1. 一种方法，包括:

建立受保护在线服务器以支持来自客户端计算机系统的密钥检索请求;

生成供安全密钥检索处理使用的密钥服务公共/私有密钥对;

生成用于装置的伪随机值;

生成与该装置相关的加密的数据结构，该加密的数据结构包括私有密钥;

基于伪随机值生成用于加密的数据结构的标识符;

在受保护在线服务器上存储该标识符和加密的数据结构; 以及

将伪随机值和密钥服务公共密钥的散列值存储到该装置内的非易失性存储器中。

2. 权利要求1所述的方法，还包括生成用于一类装置的直接证明族密钥对。

3. 权利要求2所述的方法，其中该私有密钥包括与直接证明族密钥对的公共密钥相关的直接证明私有密钥，以及该方法还包括散列直接证明私有密钥来产生私有密钥摘要。

4. 权利要求1所述的方法，还包括基于用于该装置的伪随机值而生成对称密钥。

5. 权利要求4所述的方法，其中生成标识符包括利用对称密钥加密数据值。

6. 权利要求4所述的方法，还包括利用对称密钥加密该数据结构。

7. 权利要求1所述的方法，还包括在制造受保护系统上存储密钥服务公共密钥。

8. 权利要求1所述的方法，其中用于该装置的伪随机值是唯一的。

9. 一种物品，包括具有多个机器可读指令的第一存储介质，其中当处理器执行该指令时，该指令提供以下操作:

建立受保护在线服务器以支持来自客户端计算机系统的密钥检索请求;

生成供安全密钥检索处理使用的密钥服务公共/私有密钥对;

生成用于装置的伪随机值;

生成与该装置相关的加密的数据结构，该加密的数据结构包括私

有密钥;

基于伪随机值生成用于加密的数据结构的标识符;

在受保护在线服务器上存储该标识符和加密的数据结构;以及

将伪随机值和密钥服务公共密钥的散列值存储到该装置内的非易失性存储器中。

10. 权利要求9所述的物品,还包括用于生成用于一类装置的直接证明族密钥对的指令。

11. 权利要求10所述的物品,其中该私有密钥包括与直接证明族密钥对的公共密钥相关的直接证明私有密钥,以及该物品还包括用于散列直接证明私有密钥来产生私有密钥摘要的指令。

12. 权利要求9所述的物品,还包括用于基于该装置的伪随机值而生成对称密钥的指令。

13. 权利要求12所述的物品,其中用于生成标识符的指令包括用于利用对称密钥加密数据值的指令。

14. 权利要求12所述的物品,还包括用于利用对称密钥加密该数据结构的指令。

15. 权利要求9所述的物品,还包括用于在制造受保护系统上存储密钥服务公共密钥的指令。

16. 权利要求9所述的物品,其中用于该装置的伪随机值是唯一的。

17. 一种方法,包括:

确定与安装在计算机系统中的装置相关的包括私有密钥的加密的数据结构是否被存储在该计算机系统的存储器中;以及

如果没有存储该加密的数据结构,就从该计算机系统可访问的受保护在线服务器中获得与该装置相关的加密的数据结构,该服务器存储加密的数据结构的数据库。

18. 权利要求17所述的方法,其中获得加密的数据结构包括向该装置发出获取密钥命令以启动私有密钥获取过程。

19. 权利要求17所述的方法,其中该私有密钥包括直接证明私有密钥,该直接证明私有密钥与用于一类装置的直接证明族密钥对的公共密钥相关。

20. 权利要求18所述的方法,其中私有密钥获取过程包括通过该装

置获得密钥服务公共密钥，该密钥服务公共密钥由来自受保护在线服务器的相应的密钥服务私有密钥进行签名。

21. 权利要求20所述的方法，其中私有密钥获取过程还包括基于在该装置中存储的唯一的伪随机值而生成对称密钥，以及基于该伪随机值而生成用于加密的数据结构的装置标识符。

22. 权利要求21所述的方法，其中私有密钥获取过程还包括：通过该装置生成瞬时对称密钥，建立包括装置标识符和瞬时对称密钥的检索密钥消息，利用密钥服务公共密钥来加密该检索密钥消息，以及向受保护在线服务器发送加密的检索密钥消息。

23. 权利要求22所述的方法，其中私有密钥获取过程还包括利用密钥服务私有密钥对加密的检索密钥消息进行解密，以获得装置标识符。

24. 权利要求23所述的方法，其中私有密钥获取过程还包括：对于在加密的数据结构的数据库中通过与生成的装置标识符匹配的标识符所索引的条目来搜索受保护在线服务器，在该条目中建立包括加密的数据结构的密钥响应消息，利用瞬时对称密钥加密该密钥响应消息，以及向该装置传送该密钥响应消息。

25. 权利要求24所述的方法，其中私有密钥获取过程还包括通过该装置利用瞬时对称密钥对加密的密钥响应消息进行解密，以获得加密的数据结构。

26. 权利要求25所述的方法，其中私有密钥获取过程还包括利用对称密钥对从受保护在线服务器接收的加密的数据结构进行解密，以获得私有密钥和私有密钥摘要。

27. 权利要求25所述的方法，其中私有密钥获取过程还包括散列该私有密钥以生成新的私有密钥摘要，比较来自该解密的数据结构的私有密钥摘要和新的私有密钥摘要，以及当摘要匹配时，把该私有密钥视作对该装置有效。

28. 一种物品，包括具有多个机器可读指令的存储介质，其中当由处理器执行该指令时，该指令通过以下操作来提供用于获得安装在计算机系统中的装置的私有密钥的操作：

确定与安装在计算机系统中相关的包括私有密钥的加密的数据结构是否被存储在该计算机系统的存储器中；以及

如果没有存储加密的数据结构，就从该计算机系统可访问的受保护在线服务器中获得与该装置相关的加密的数据结构，该服务器存储加密的数据结构的数据库。

29. 权利要求28所述的物品，其中用于获得加密的数据结构的指令包括用于向该装置发出获取密钥命令以启动私有密钥获取过程的指令。

30. 权利要求28所述的物品，其中该私有密钥包括直接证明私有密钥，该直接证明私有密钥与用于一类装置的直接证明族密钥对的公共密钥相关。

31. 权利要求29所述的物品，其中用于私有密钥获取过程的指令包括用于通过该装置获得密钥服务公共密钥的指令，该密钥服务公共密钥由来自受保护在线服务器的相应的密钥服务私有密钥进行签名。

32. 权利要求31所述的物品，其中用于私有密钥获取过程的指令还包括用于基于在该装置中存储的唯一的伪随机值而生成对称密钥、以及基于该伪随机值而生成用于加密的数据结构的装置标识符的指令。

33. 权利要求32所述的物品，其中用于私有密钥获取过程的指令还包括用于以下操作的指令：通过该装置生成瞬时对称密钥，建立包括装置标识符和瞬时对称密钥的检索密钥消息，利用密钥服务公共密钥来加密该检索密钥消息，以及向受保护在线服务器发送加密的检索密钥消息。

34. 一种用于使用安全协议向安装在客户端计算机系统中的装置传递私有密钥的系统，包括：

受保护在线服务器，其可由客户端计算机系统访问，并被配置成生成密钥服务公共/私有密钥对，存储加密的数据结构的数据库，每个加密的数据结构包括与选定的装置对应的私有密钥，以及将加密的数据结构中所选定的数据结构安全地传送给该装置；

受保护系统，其被耦合到该受保护服务器，并被配置成生成与该装置相关的加密的数据结构，接收来自该受保护服务器的密钥服务公共密钥，以及向受保护在线服务器发送该加密的数据结构；以及

生产系统，其被耦合到该受保护系统，并被配置成接收来自受保护系统的密钥服务公共密钥的散列值和唯一的伪随机值，以及在向客户端计算机系统中安装该装置之前，将该密钥服务公共密钥的散列值

和唯一的伪随机值存储到该装置的非易失性存储器中。

35. 权利要求 34 所述的系统，其中私有密钥包括与直接证明族密钥对的公共密钥相关的直接证明私有密钥。

利用在线服务向装置传递直接证明私有密钥的方法

背景

1. 领域

本发明一般而言涉及计算机安全，更具体而言，涉及向处理系统中的装置安全地分发密钥。

2. 描述

一些支持内容保护和/或计算机安全特性的处理系统架构要求，专门保护的或“可信的”软件模块能够创建与处理系统中特定的受保护或“可信的”硬件装置（举例来说，例如图形控制器卡）经过验证的加密的通信会话。一种通常用来标识该装置并同时建立该加密的通信会话的方法是使用单侧验证的 Diffie-Helman（DH）密钥交换过程。在该过程中，向该装置分配唯一的公共/私有 Rivest、Shamir 和 Adelman（RSA）算法密钥对或唯一的椭圆曲线密码术（ECC）密钥对。然而，由于该验证过程使用 RSA 或 ECC 密钥，所以该装置于是具有一个唯一且可证明的身份（identity），这会引起对保密的担心。在最坏的情况下，这些担心会导致缺乏来自用于建立提供这类安全性的可信装置的原始设备制造商（OEM）的支持。

附图简述

根据本发明的以下详细说明，本发明的特征和优点将变得显而易见，其中：

图 1 说明一种系统，该系统的特征在于利用根据本发明一个实施例进行操作的可信平台模块（TPM）来实施的平台；

图 2 说明包括图 1 的 TPM 的平台的第一实施例；

图 3 说明包括图 1 的 TPM 的平台的第二实施例；

图 4 说明利用图 2 的 TPM 来实施的计算机系统的示例性实施例；

图 5 是根据本发明实施例用于利用在线服务向装置分发直接证明（Direct Proof）密钥的系统的图；

图 6 是说明根据本发明实施例利用在线服务分发直接证明密钥的方法的阶段的流程图；

图 7 是说明根据本发明实施例的受保护服务器建立处理的流程图；

图 8 是说明根据本发明实施例的装置制造商建立处理的流程图；

图 9 是说明根据本发明实施例的装置制造商生产处理的流程图；

图 10-12 是根据本发明实施例的客户端计算机系统建立处理的流程图；以及

图 13 是根据本发明实施例的客户端计算机系统处理的流程图。

详细描述

利用基于直接证明的 Diffie-Helman 密钥交换协议来允许受保护/可信装置验证自己并建立与可信软件模块的加密的通信会话，避免了在处理系统中创建任何唯一的身份信息，从而避免带来对保密的担心。然而，在生产线上的装置中直接嵌入直接证明私有密钥对于该装置比其他方法要求更多的受保护非易失性存储，从而增加了装置成本。本发明的一个实施例是一种利用在线服务以安全的方式允许直接证明（DP）私有密钥（例如用于签名）被传递给装置并随后由装置本身安装在装置中的方法。在本发明中所给出的该方法被设计成使得该装置无需泄露用于安装过程的身份信息。在一个实施例中，支持该能力所需的装置存储的减少可以从大约 300 至 700 个字节下降到大约 40 个字节。实施用于装置的基于直接证明的 Diffie-Helman 密钥交换所需的非易失性存储量的该减少会导致更广泛地采用该技术。

在本发明的实施例中，不在装置中或利用装置来分发 DP 私有签名密钥。代之以，该装置支持这样一种协议，通过该协议，现场的装置可以安全地从由制造商或供应商或代表所提供的在线受保护服务器中检索它的私有密钥。该协议在装置与服务器之间创建可信通道，并且不需要信任任何介入（intervening）软件，包括在本地处理系统上的软件。

在说明书中对本发明的“一个实施例”或“实施例”的引用意味着，在本发明的至少一个实施例中包含结合该实施例所描述的特定特性、结构或特征。因此，在整个说明书的各种位置出现的短语“在一个实施例中”未必都指相同的实施例。

在以下的描述中，利用某个术语来描述本发明一个或多个实施例

的某些特征。例如，“平台”被定义为适于发送和接收信息的任何类型的通信装置。各种平台的实例包括但不限制或局限于计算机系统、个人数字助理、蜂窝电话、机顶盒、传真机、打印机、调制解调器、路由器等等。“通信链路”被广泛地定义为适于平台的一个或多个信息承载介质。各种类型的通信链路的实例包括但不限制或局限于电线、光纤、电缆、总线轨迹（trace）、或无线信令技术。

“询问器”是指向另一实体请求对真实性或权限进行某种检验的任何实体（例如人、平台、系统、软件和/或装置）。通常，这在公开或提供所请求的信息之前执行。“应答器”是指已被请求提供对其权限、有效性和/或身份进行某种证明的任何实体。可与“认证制造商”互换使用的“装置制造商”是指制造或配置平台或装置的任何实体。

如在此所使用，向询问器“证明”或“确信”应答器已经拥有或知道某种密码信息（例如数字签名、诸如密钥之类的秘密等）意味着，基于向询问器所公开的该信息与证明，该应答器非常可能具有该密码信息。向询问器证明这一点而不用向该询问器“泄露”或“公开”该密码信息意味着，基于向询问器公开的该信息，对于询问器而言确定该密码信息在计算上将是不可行的。

在下文中将这种证明称为直接证明。术语“直接证明”是指零知识证明，因为这些类型的证明在本领域中通常是已知的。特别地，在此所引用的特定直接证明协议是2002年11月27日提交的、转让给本申请的所有者的、顺序号为10/306,336、标题为“System and Method for Establishing Trust Without Revealing Identity”的同时待审的专利申请的主题。直接证明定义了一种协议，在该协议中发行者定义一个许多成员的族（family），这些成员共享如由该发行者所定义的公共特征。该发行者生成一个族公共和私有密钥对（Fpub和Fpri），其总体上表示该族。利用 Fpri，发行者还可以为该族中的每个单独成员生成一个唯一的直接证明私有签名密钥（DPpri）。可以利用该族公共密钥Fpub来检验由单独的 DPpri 所签名的任何消息。然而，这样的检验只是识别该签名者是该族的一个成员；没有揭露关于单独的成员的唯一的识别信息。在一个实施例中，发行者可以是装置制造商或代表。也就是，发行者可以是具有下述能力的实体：基于共享的特征来定义装置族，产生族公共/私有密钥对，以及创建DP私有密钥并将其注入到装置中。

发行者还可以生成用于该族公共密钥的证书，其识别该密钥的来源和该装置族的特征。

现在参考图 1，示出了一个系统的实施例，其特征在于利用根据本发明的一个实施例进行操作的可信硬件装置（称为“可信平台模块”或“TPM”）来实施的平台。第一平台 102（询问器）发送请求 106，即请求第二平台 104（应答器）提供关于它自己的信息。响应于请求 106，第二平台 104 提供所请求的信息 108。

另外，为了提高安全性，第一平台 102 可能需要检验来自由一个选定的装置制造商或一组选定的制造商（在下文中称为“装置制造商 110”）制造的装置所请求的信息 108。例如，对于本发明的一个实施例，第一平台 102 询问第二平台 104 以显示它具有由装置制造商 110 所产生的密码信息（例如签名）。可以将该询问结合到请求 106（如所示）中或分开发送。第二平台 104 通过以应答的形式提供信息来应答该询问，以使第一平台 102 确信第二平台 104 具有由装置制造商 110 所产生的密码信息，而不用泄露该密码信息。该应答可以是所请求的信息 108（如所示）的一部分或分开发送。

在本发明的一个实施例中，第二平台 104 包括可信平台模块（TPM）115。TPM 115 是由装置制造商 110 所制造的密码装置。在本发明的一个实施例中，TPM 115 包括具有密封在封装内的少量片上存储器的处理器。将 TPM 115 配置成向第一平台 102 提供信息，该信息将使它能够确定应答是从有效的 TPM 发送的。所用的信息是将使得不大可能确定 TPM 的或第二平台的身份的内容。

图 2 说明具有 TPM 115 的第二平台 104 的第一实施例。对于本发明的该实施例，第二平台 104 包括耦合到 TPM 115 的处理器 202。通常，处理器 202 是处理信息的装置。例如，在本发明的一个实施例中，处理器 202 可以被实施为微处理器、数字信号处理器、微控制器或者甚至状态机。可选择地，在本发明的另一个实施例中，处理器 202 可以被实施为可编程或硬编码逻辑，例如现场可编程门阵列（FPGA）、晶体管-晶体管逻辑（TTL）逻辑、或者甚至是专用集成电路（ASIC）。

在此，第二平台 104 还包括存储单元 206 以允许存储密码信息，例如以下的一种或多种：密钥、散列值、签名、证书等等。可以将散列值“X”表示为“Hash(X)”。预期这样的信息可以被存储在 TPM 115

的内部存储器 220 内以代替如图 3 所示的存储单元 206。可以对密码信息进行加密，尤其是在 TPM 115 外部存储该信息的时候。

图 4 说明了包括利用图 2 的 TPM 115 所实施的计算机系统 300 的平台的实施例。计算机系统 300 包括总线 302 和耦合到总线 302 的处理器 310。计算机系统 300 还包括主存储单元 304 和静态存储单元 306。

在此，主存储单元 304 是用于存储由处理器 310 执行的信息和指令的易失性半导体存储器。主存储器 304 还可用于存储在处理器 310 执行指令期间的临时变量或其它中间信息。静态存储单元 306 是用于以更永久的特性存储处理器 310 的信息和指令的非易失性半导体存储器。静态存储器 306 的实例包括但不限制或局限于只读存储器（ROM）。主存储单元 304 和静态存储单元 306 都被耦合到总线 302。

在本发明的一个实施例中，计算机系统 300 还包括数据存储装置 308，例如磁盘或光盘，并且它对应的驱动器还可以被耦合到计算机系统 300 以用于存储信息和指令。

计算机系统 300 还可以通过总线 302 被耦合到图形控制器装置 314，该图形控制器装置 314 控制用于向终端用户显示信息的显示器（未示出），该显示器例如是阴极射线管（CRT）、液晶显示器（LCD）或任何平板显示器。在一个实施例中，可能期望该图形控制器能够建立与由处理器所执行的软件模块的经过验证的加密通信会话。

典型地，字母数字输入装置 316（例如键盘、小键盘等）可以被耦合到总线 302 以用于将信息和/或命令选择传送给处理器 310。另一种类型的用户输入装置是光标控制单元 318，例如鼠标、轨迹球、触摸板、触笔或光标方向键，用于将方向信息和命令选择传送给处理器 310 以及用于控制显示器 314 上的光标移动。

通信接口单元 320 还被耦合到总线 302。接口单元 320 的实例包括调制解调器、网络接口卡、或者其它众所周知的用于耦合到形成局域网或广域网的一部分的通信链路的接口。以这种方式，计算机系统 300 可以通过常规网络基础设施被耦合到多个客户端和/或服务器，该网络基础设施例如是公司的内部网和/或因特网。在一个实施例中，计算机系统可以通过网络被在线耦合到受保护的服务器。

认识到的是，对于某些实施而言，可能期望比上述更少或更多的配备的计算机系统。因此，计算机系统 300 的配置将根据实施情况而

发生变化，这取决于多个因素，例如价格约束、性能要求、技术改进、和/或其它情况。

在至少一个实施例中，计算机系统 300 可以支持专门保护的“可信”软件模块（例如抗篡改软件、或具有运行受保护程序的能力的系统）的使用，该“可信”软件模块被存储在主存储器 304 和/或大容量存储装置 308 中，并由处理器 310 执行以进行特定活动，即使在该系统中存在其它恶意软件。这些可信软件模块中的一些同样要求不仅仅对其它平台进行“可信的”受保护访问，还对相同平台内一个或多个外围装置进行该访问，例如图形控制器 314。通常，这些访问要求该可信软件模块能够识别该装置的能力和/或特定身份，然后建立与该装置的加密的会话以允许数据的交换，该系统中的其它软件无法窥探或欺骗该数据交换。

现有技术中一种识别该装置并同时建立加密的会话的方法是使用单侧验证的 Diffie-Hellman（DH）密钥交换过程。在该过程中，向该装置分配唯一的公共/私有 RSA 或 ECC 密钥对。该装置拥有和保护该私有密钥，同时可以向软件模块发布公共密钥以及验证证书。在 DH 密钥交换过程期间，该装置利用它的私有密钥签名一个消息，该软件模块可以利用对应的公共密钥来检验该消息。这允许软件模块验证该消息实际上的确来自感兴趣的装置。

然而，由于该验证过程使用了 RSA 或 ECC 密钥，所以该装置具有一个唯一且可证明的身份。可以使该装置利用它的私有密钥来签名一个消息的任何软件模块都可以证明在计算机系统中存在该特定的唯一装置。假定装置很少在处理系统之间移动，那么这还表示一个可证明的唯一计算机系统身份。此外，该装置的公共密钥本身表示恒定的唯一值；实际上是永久的“cookie”。有时，可以把这些特征解释为一个显著的保密问题。

在 2004 年提交的、转让给本申请的所有者的、标题为“An Apparatus and Method for Establishing an Authenticated Encrypted Session with a Device Without Exposing Privacy-Sensitive information”、顺序号为 10/???,???的同时待审的专利申请中描述了一种可选方法。在该方法中，用直接证明密钥来代替在单端验证的 Diffie-Helman 过程中使用的 RSA 或 ECC 密钥。可以将使用该方法的

装置验证为属于特定装置族，这可以包括保证关于该装置的特性或可信赖度。该方法并未揭露任何可以用来建立一个表示该处理系统的唯一身份的唯一识别信息。

尽管该方法工作良好，但是它要求在该装置中的附加存储来保存直接证明私有密钥，该密钥可以大于 RSA 或 ECC 密钥。为了减轻该附加存储要求的负担，本发明的实施例限定了一种用于确保该装置在它需要直接证明私有密钥时具有该密钥而不用要求该装置中相当大的附加存储的系统和过程。

在本发明的至少一个实施例中，装置制造商向生产线的装置中存储一个 128 位的伪随机数，并且可以对一个大得多的直接证明私有密钥（DPpri）进行加密，以及利用由受保护服务器所操作的在线服务将其传递给现场的装置。其它实施例可以向该装置中存储一个比 128 位更长或更短的数字。该过程确保只有一个指定的装置可以解密和使用它的分配的 DPpri 密钥。图 5 是根据本发明实施例用于分发直接证明密钥的系统 500 的图。在该系统中有四个实体：装置制造受保护系统 502、装置制造生产系统 503、客户端计算机系统 504 和受保护服务器 522。装置制造受保护系统包括用在装置 506 的制造之前的建立过程中的处理系统。该制造受保护系统 502 可由装置制造商操作，使得保护受保护系统免遭来自装置制造地点（例如它是封闭系统）外部的黑客的攻击。制造生产系统 503 可以用在装置的制造过程中。在一个实施例中，该受保护系统和生产系统可以是相同的系统。装置 506 包括任何包含在客户端计算机系统中的硬件装置（例如存储器控制器、外围装置比如图形控制器、I/O 装置等等）。在本发明的实施例中，该装置包括存储在该装置的非易失性存储器中的伪随机值 RAND 508 和密钥服务公共密钥散列值 509。

该制造受保护系统包括受保护数据库 510 和生成函数 512。该受保护数据库包括用于存储由生成函数 512 以如下所述的方式产生的多个伪随机值（至少与将制造的每个装置的一样多）的数据结构。该生成函数包括产生在此被称为密钥块（keyblob）514 的数据结构的逻辑（以软件或硬件来实施）。密钥块 514 包括至少三个数据项。唯一直接证明私有密钥（DPpri）包括可由装置用于进行签名的密钥。DP 私有摘要 516（DPpri 摘要）包括根据产生保密消息摘要的任何公知方法例如

SHA-1 的 DPpri 的消息摘要。一些实施例可以包括伪随机初始化向量（IV）518，该向量包括作为密钥块的一部分的比特流以用于兼容性目的。如果流密码被用于加密，则以使用流密码中的 IV 的公知方法来使用 IV。如果将块密码用于加密，则 IV 将被用作待加密的消息的一部分，因此使该加密的每个实例都不相同。该制造受保护系统还包括用于在线协议的密钥服务公共密钥 507，正如以下进一步详细描述的。

在本发明的实施例中，该制造受保护系统产生一个或多个密钥块（如以下详细描述的），并在受保护服务器 522 上的密钥块数据库 520 中存储该密钥块。在一个实施例中，在密钥块数据库中可以有许多密钥块。可由装置制造商、装置分发商或其它附属实体来操作该受保护服务器。该受保护服务器可以利用网络比如因特网被可通信地耦合到客户端计算机系统 504。该受保护服务器还包括密钥服务私有密钥 511，其用于在受保护服务器和该装置之间的在线协议。

客户端计算机系统 504 期望使用直接证明协议以用于验证以及与系统 504 内包含的装置 506 进行通信会话的密钥交换，该客户端计算机系统 504 可以利用密钥服务公共/私有密钥对和以下进一步描述的在线协议来从受保护服务器上的密钥块数据库 520 中读取一个选定的密钥块 514。可由该装置使用该密钥块数据来产生一个本地化密钥块 524（如下所述），以用于实施直接证明协议。由客户端计算机系统来执行装置驱动器软件 526 以初始化并控制装置 506。

在本发明的实施例中，存在五个不同的操作阶段。图 6 是说明根据本发明实施例的分发直接证明密钥的方法的阶段的流程图 600。根据本发明的实施例，可以在每个阶段执行某些动作。在装置制造商的地点，至少存在三个阶段：受保护服务器建立阶段 601、装置制造商建立阶段 602 和装置制造商生产阶段 604。在此参考图 7 来描述该受保护服务器建立阶段。在此参考图 8 来描述该装置制造商建立阶段。在此参考图 9 来描述该装置制造商生产阶段。在具有客户端计算机系统的消费者地点，至少存在两个阶段：客户端计算机系统建立阶段 606 和客户端计算机系统使用阶段 608。在此参考图 10-12 来描述该客户端计算机系统建立阶段。在此参考图 13 来描述该客户端计算机系统使用阶段。

图 7 是说明根据本发明实施例的受保护服务器建立阶段处理的流

程图 700。可以在生产装置之前由装置制造商执行该处理。在块 702，装置制造商建立一个受保护服务器 522 来支持密钥检索请求。在一个实施例中，该受保护服务器以公知的方式被可通信地耦合到因特网。为了提高安全性，该受保护服务器不应当与在制造受保护系统或制造生产系统中使用的处理系统相同。在块 704，装置制造商产生一个密钥服务公共/私有密钥对，该密钥对将用于由受保护服务器所提供的密钥检索服务。在一个实施例中，可以在受保护服务器中存储该密钥服务公共/私有密钥对。对于由该系统执行的所有处理可以只产生一次该密钥对，或者对每类装置产生一个新的密钥对。在块 706，该装置制造商将密钥服务公共密钥 507 传递给制造受保护系统 502。

图 8 是说明根据本发明实施例的装置制造建立处理的流程图 800。在一个实施例中，装置制造商可以利用制造受保护系统 502 来执行这些动作。在块 802，装置制造商为每类将要制造的装置产生一个直接证明族密钥对（Fpub 和 Fpri）。每个唯一的装置将具有一个 DPpri 密钥，以使可由 Fpub 检验利用 DPpri 产生的签名。一类装置可以包括任何装置集合或子集，例如一个选定的生产线（即装置的类型）或基于版本号的一个生产线的子集、或装置的其它特征。该族密钥对是由产生其的装置类使用。

对于每个将要制造的装置，制造受保护系统 502 的生成函数 512 执行块 804 至 820。首先，在块 804，该生成函数产生一个唯一的伪随机值（RAND）508。在一个实施例中，RAND 的长度是 128 比特。在其它实施例中，可以使用其它大小的值。在一个实施例中，可以提前产生多个装置的伪随机值。在块 806，利用该装置所支持的单向函数 f，该生成函数根据唯一的 RAND 值（SKEY=f（RAND））产生一个对称的加密密钥 SKEY。该单向函数可以是适用于该目的的任何已知算法（例如 SHA-1、MGF1、数据加密标准（DES）、三重 DES、高级加密标准（AES）等）。在块 808，在一个实施例中，该生成函数产生一个标识符（ID）标签，它将用来在受保护服务器 522 上的密钥块数据库 520 中引用该装置的密钥块 514，通过利用 SKEY 来加密一个“空输入”（例如少量的零字节）（装置 ID=利用 SKEY 加密（0...0））。在其它实施例中，可以使用产生该装置 ID 的其它方式，或者可以由 SKEY 对其它值进行加密。

接下来，在块 810，该生成函数产生与该装置的族密钥对（Fpub）相关的 DP 私有签名密钥 DPpri。在块 812，该生成函数利用已知的方法（例如利用 SHA-1 或另一散列算法）对 DPpri 进行散列以产生 DPpri 摘要。在块 814，该生成函数为该装置创建密钥块数据结构。该密钥块包括至少 DPpri 和 DPpri 摘要。在一个实施例中，该密钥块还包括具有多个伪随机产生的比特的随机初始化向量。可以利用 SKEY 对这些值进行加密以产生加密的密钥块 514。在块 816，可以在密钥块数据库 520 的条目（entry）中存储在块 808 产生的装置 ID 和在块 814 产生的加密密钥块 514。在一个实施例中，可由装置 ID 来表示在密钥块数据库中的该条目。在块 818，可以在受保护数据库 510 中存储当前 RAND 值。在块 820，可以删除 SKEY 和 DPpri，因为它们将由现场的装置再生。

DPpir 摘要的创建和随后利用 SKEY 的加密被设计成使得，任何不拥有 SKEY 的实体无法确定 DPpri 的内容，以及任何不拥有 SKEY 的实体不能修改密钥块的内容，而没有随后由的确拥有 SKEY 的实体进行检测。在其它实施例中，可以使用用于提供该保密和完整性保护的其它方法。在一些实施例中，可能不要求该完整性保护，并且可以使用仅仅提供保密的方法。在这种情况下， DPpri 摘要的值将不是必需的。

在块 820 之后的任何时候，在块 822，可以安全地将受保护的 RAND 值的数据库上载到制造生产系统 503，该制造生产系统 503 将在制造过程期间向该装置中存储 RAND 值。一旦检验了该上载，就可以安全地从制造受保护系统 502 中删除 RAND 值。最后，在块 824，可以在受保护服务器 522 上存储具有多个加密密钥块的密钥块数据库 520，其中对于每个装置将使用一个密钥块数据库条目，正如由装置 ID 字段所索引的。

图 9 是说明根据本发明实施例的装置制造生产处理的流程图 900。当在生产线中制造装置时，在块 902，该制造生产系统从受保护数据库中选择一个未使用的 RAND 值。于是可以向装置的非易失性存储器中存储该选定的 RAND 值。在一个实施例中，该非易失性存储器包括 TPM。在一个实施例中，可以在大约为 16 个字节的非易失性存储器中存储该 RAND 值。在块 904，可以在该装置的非易失性存储器中存储

该密钥服务公共密钥 507 的散列 509。可以利用任何已知的散列算法来产生该散列。在一个实施例中，可以在大约为 20 个字节的非易失性存储器中存储该散列值。在块 906，一旦该 RAND 值的存储是成功的，那么该制造生产系统就销毁在受保护数据库 510 中该装置的 RAND 的任何记录。在此，在该装置中存储该 RAND 值的唯一副本。

在可选择的实施例中，可以在制造装置的过程中创建该 RAND 值，然后发送到制造受保护系统以用于密钥块的计算。

在另一个实施例中，可以在该装置上创建该 RAND 值，以及该装置和该制造受保护系统可以参加利用不在该装置的外部泄露 DPpri 密钥的方法来产生该 DPpri 密钥的协议。然后该装置可以创建装置 ID、SKEY 和密钥块。该装置将把装置 ID 和密钥块传送到制造系统以用于在受保护数据库 510 中进行存储。在该方法中，制造系统在受保护数据库中以相同的信息（装置 ID、密钥块）来结束，但是不知道 RAND 的值或 Dppri 的值。

图 10-12 是根据本发明实施例的客户端计算机系统建立处理的流程图。客户端计算机系统可以执行作为启动该系统的一部分的这些动作。从图 10 的流程 1000 开始，在块 1002，可以以正常方式启动客户端计算机系统，并将该装置的装置驱动器软件模块 526 加载到客户端计算机系统的主存储器中。当该装置驱动器被初始化并开始执行时，在块 1004，该装置驱动器确定是否已经存在在装置 506 的大容量存储器装置 308 中存储的加密的本地化密钥块 524。如果存在，就不必执行进一步的建立处理，该建立处理在块 1006 处结束。如果不存在，就在块 1008 继续进行该处理。在块 1008，该装置驱动器向装置 506 发出一个获取密钥命令来启动该装置的 DP 私有密钥获取过程。

在块 1010，该装置驱动器向该装置发送密钥服务公共密钥 507。在块 1014，该装置提取接收的密钥服务公共密钥，产生该密钥服务公共密钥的散列值，以及比较所接收的密钥服务公共密钥的散列与存储在该装置的非易失性存储器中的密钥服务公共密钥散列 509。如果该散列匹配，就知道所接收的密钥服务公共密钥是装置制造商的密钥检索服务的密钥服务公共密钥，并且继续进行客户端计算机系统建立处理。

在另一个实施例中，该装置可以接收一个认证的密钥服务公共密

钥的证书，可以通过到密钥服务公共密钥的一个证书链来检验该证书，该密钥服务公共密钥的散列是存储在该装置的非易性存储器中的密钥服务公共密钥散列 509。然后在后续步骤中可以将该认证的密钥服务公共密钥用作密钥服务公共密钥。

在块 1018，该装置使用它的单向函数 f 来从嵌入的 RAND 值 508 中再生该对称密钥 SKEY（SKEY=f（RAND））。然后在块 1020，该装置通过利用 SKEY 来加密一个“空输入”（例如少量的零字节）（装置 ID=利用 SKEY 来加密（0...0）），从而产生它的唯一的装置 ID 标签。根据图 11 的流程图 1100 继续进行该处理。

在图 11 的块 1102，该装置产生一个瞬时对称密钥 Tkey。该密钥将被发送到受保护服务器，该受保护服务器可以使用该密钥来加密受保护服务器返回到该装置的消息。在块 1104，该装置建立包含装置 ID 和瞬时对称密钥 Tkey 的检索密钥请求消息，利用在块 1014 从装置驱动器接收的密钥服务公共密钥来加密该消息，然后通过装置驱动器向受保护服务器发送检索密钥请求消息。（检索密钥请求=利用密钥服务公共密钥来加密（装置 ID，Tkey））。本领域技术人员将认识到，为了利用公共密钥来加密消息，通常将为对称密码创建会话密钥（Skey），利用公共密钥加密该会话密钥，然后利用该会话密钥加密该消息。在块 1106，受保护服务器利用密钥服务私有密钥 511 来解密所接收的密钥请求消息，然后提取在此存储的字段。由于受保护服务器现在知道该装置 ID（从密钥请求消息中获得），所以受保护服务器在密钥块数据库中搜索包含该匹配装置 ID 值的记录，以及从该记录中提取该装置的加密的密钥块。在块 1110，该受保护服务器建立一个包含族公共密钥和加密的密钥块的第二响应消息，并利用由该装置所提供的瞬时对称密钥 Tkey 来加密该第二响应消息。因此，密钥响应=（族公共密钥，利用 Tkey 加密（加密的密钥块））。利用 Tkey 对该加密的密钥块进行加密并不是要保护该密钥块，因为已经利用对称密钥 SKEY 加密了该密钥块，只有该装置可以再生该密钥块。更确切地说，以这种方式加密消息确保了返回的密钥块在每次执行该密钥获取过程时都进行改变，因此确保了该密钥块本身不能用作“cookie”。可以在块 1112 将第二响应消息返回到客户端计算机系统上的装置驱动器，该装置驱动器向该装置转发该消息。

在块 1114，该装置从第二响应消息中提取族公共密钥，利用瞬时对称密钥 Tkey 对该打包的密钥块进行解密，以及在该装置的易失性存储器中存储该加密的密钥块。然后以图 12 的流程图 1200 继续进行该处理。

在图 12 的块 1216，该装置利用对称密钥 SKEY 对加密的密钥块进行解密以产生 DPpri 和 DPpri 摘要，并在其非易失性存储器中存储这些值（解密的密钥块=利用 SKEY 解密（ IV，DPpri，DPpri 摘要））。可以丢弃该初始化向量（IV）。然后在块 1218，该装置通过使 DPpri 散列并比较该结果与 DPpri 摘要来检查 DPpri 的完整性。如果该比较是好的，该装置就接受 DPpri 作为它的有效密钥。该装置在一个实施例中还可以将密钥获取的标志设置成真来表示已经成功地获取了 DP 私有密钥。在块 1220，该装置选择一个新的 IV，并利用新的 IV 创建一个新的加密的本地化密钥块（本地化密钥块=利用 SKEY 加密（IV2，DPpri，DPpri 摘要））。在一个实施例中，可以将该新的加密的本地化密钥块返回到客户端计算机系统上的密钥检索实用程序（utility）软件模块（未在图 5 中示出）。在块 1222，该密钥检索实用程序在客户端计算机系统内的存储器中存储该加密的本地化密钥块（例如大容量存储装置 308）。现在在客户端计算机系统中安全地存储该装置的 DPpri。

一旦该装置在建立处理期间获取了 DPpri，该装置就可以使用 DPpri。图 13 是根据本发明实施例的客户端计算机系统处理的流程图 1300。该客户端计算机系统可以在已经完成了该建立之后的任何时候执行这些动作。在块 1302，可以以正常方式启动客户端计算机系统，并可以将该装置的装置驱动器 526 加载到主存储器中。当该装置驱动器被初始化并开始执行时，该装置驱动器确定是否已经存在在该装置 506 的大容量存储器装置 308 中存储的加密的本地化密钥块 524。如果不存在，则执行图 10-12 的建立处理。如果对于该装置存在可用的加密的本地化密钥块，则利用块 1306 继续进行该处理。在块 1306，该装置驱动器检索加密的本地化密钥块，并向该装置传送该密钥块。在一个实施例中，可以通过执行一个加载密钥块命令来完成该密钥块的传送。

在块 1308，该装置利用它的单向函数 f 来从嵌入的 RAND 值 508

（SKEY=f（RAND））中再生该对称密钥（现在供解密所用）。在块1310，该装置利用对称密钥 SKEY 对加密的本地化密钥块进行解密以产生 DPpri 和 DPpri 摘要，并在其非易失性存储器中存储这些值（解密的密钥块=利用 SKEY 解密（IV2，DPpri，DPpri 摘要））。可以丢弃第二初始化向量（IV2）。在块 1312，该装置通过使 DPpri 散列并比较该结果与 DPpri 摘要来检查 DPpri 的完整性。如果该比较是好的（例如摘要匹配），该装置就接受 DPpri 作为早先获取的有效密钥，并使它能够使用。该装置还可以将一个密钥获取标志设置成真来表示已经成功地获取了 DP 私有密钥。在块 1314，该装置也选择了另一个新的 IV，并利用新的 IV 创建一个新的加密的本地化密钥块（本地化密钥块=利用 SKEY 加密（IV3，DPpri，DPpri 摘要））。可以将该新的加密的本地化密钥块返回到密钥检索实用程序。在块 1316，该密钥检索实用程序在客户端计算机系统内的存储器中存储该加密的本地化密钥块（例如大容量存储器 308）。现在在客户端计算机系统中再次安全地存储该装置的 DPpri。

在本发明的一个实施例中，不必同时产生所有的装置 DP 私有密钥。假设定期更新受保护服务器上的密钥块数据库，就可以在需要时成批地产生该装置 DP 私有密钥。该密钥块数据库每次在受保护服务器上更新时，它都将包含至今产生的密钥块数据库，包括那些已经产生但是还没有分配到装置的装置密钥。

在另一个实施例中，有可能延迟该装置的 DPpri 密钥的产生，从而允许只对需要它们的那些装置产生这些密钥。一旦接收来自该装置的第一密钥获取请求，该受保护服务器就会产生对制造受保护系统的请求，该系统仍将保存该装置的 RAND 值。此时，该制造受保护系统产生该装置的 DPpri 密钥，将它返回给受保护服务器，并只有在那时才销毁该 RAND 值。

在另一个实施例中，代替在该装置上的非易失性存储器中存储密钥服务公共密钥散列，该装置制造商可以选择存储根密钥的散列，然后利用根密钥为密钥服务公共密钥签署证书。以这种方式，相同的根密钥可以用于非常多的装置。

尽管可以将在此讨论的操作描述为一种顺序过程，但是实际上其中的一些操作可以并行或同时执行。另外，在一些实施例中，可以在

不偏离本发明精神的情况下重新安排该操作的次序。

在此描述的技术并不限于任何特定的硬件或软件配置；它们可以应用于任何计算或处理环境。可以以硬件、软件或二者的组合来实施该技术。可以以在可编程机器上执行的程序来实施该技术，所述可编程机器例如是移动或固定计算机、个人数字助理、机顶盒、蜂窝电话和寻呼机、以及其它电子装置，其每一种包括处理器、处理器可读的存储介质（包括易失性和非易失性存储器和/或存储元件）、至少一个输入装置、以及一个或多个输出装置。向利用输入装置输入的数据应用程序代码来执行所述的功能并生成输出信息。可以向一个或多个输出装置应用该输出信息。本领域技术人员可以认识到，本发明可以利用各种计算机系统配置来实行，包括多处理器系统、小型计算机、大型计算机等等。本发明还可以在分布式计算环境中实行，其中可以由通过通信网络链接的远程处理装置来执行任务。

可以以一种高级过程或面向对象的编程语言来实施每个程序以与处理系统进行通信。然而，如果期望的话，可以以汇编或机器语言来实施程序。无论如何，可以编译或解释该语言。

可以使用程序指令来使利用指令编程的通用或专用处理系统执行在此所述的操作。可选择地，可以由包含用于执行该操作的硬连线逻辑的特定硬件部件、或者由该编程的计算机部件和定制的硬件部件的任何组合来执行该操作。可以将在此所述的方法提供为一种计算机程序产品，该计算机程序产品可以包括具有存储在其上的指令的机器可读介质，该指令可以用来对处理系统或其他电子装置进行编程来执行该方法。在此使用的术语“机器可读介质”应当包括任何能够存储或编码由该机器执行的指令序列并且使该机器执行在此所述的任何一种方法的介质。因此该术语“机器可读介质”应当包括但不限于固态存储器、光盘和磁盘、以及编码数据信号的载波。此外，在本领域中常见的是把以一种形式或另一种形式的软件（例如程序、过程、进程、应用、模块、逻辑等等）说成是采取动作或导致结果。这样的表达仅仅是一种陈述对处理系统执行该软件导致该处理器执行产生结果的动作的简写方式。

尽管在此已经参考说明性实施例描述了本发明，但是该描述并不打算在限制的意义上进行解释。对于本领域技术人员而言本发明明显

适合的该说明性实施例的各种修改、以及本发明的其它实施例被视为在本发明的精神和范围内。

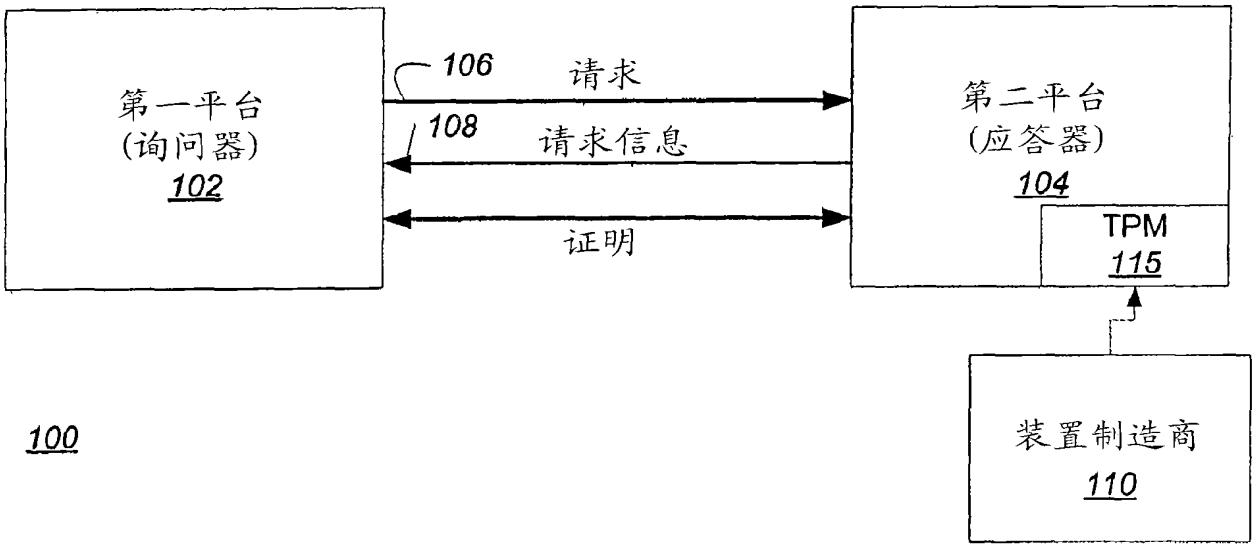

第一平台
(询问器)
102
106
请求
108
请求信息
证明
第二平台
(应答器)
104
TPM
115
装置制造商
110
100

图 1

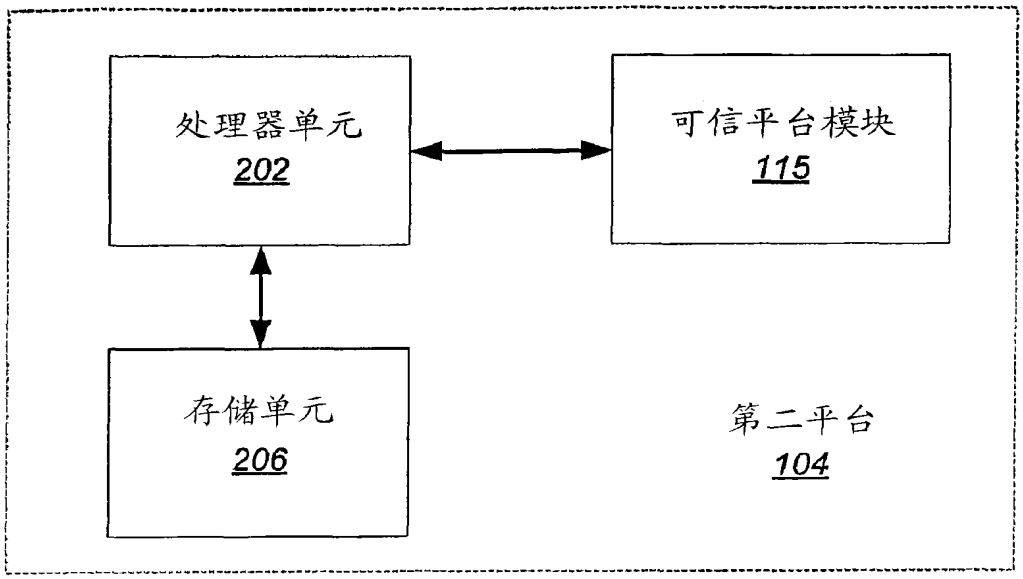

处理器单元
202
可信平台模块
115
存储单元
206
第二平台
104

图 2

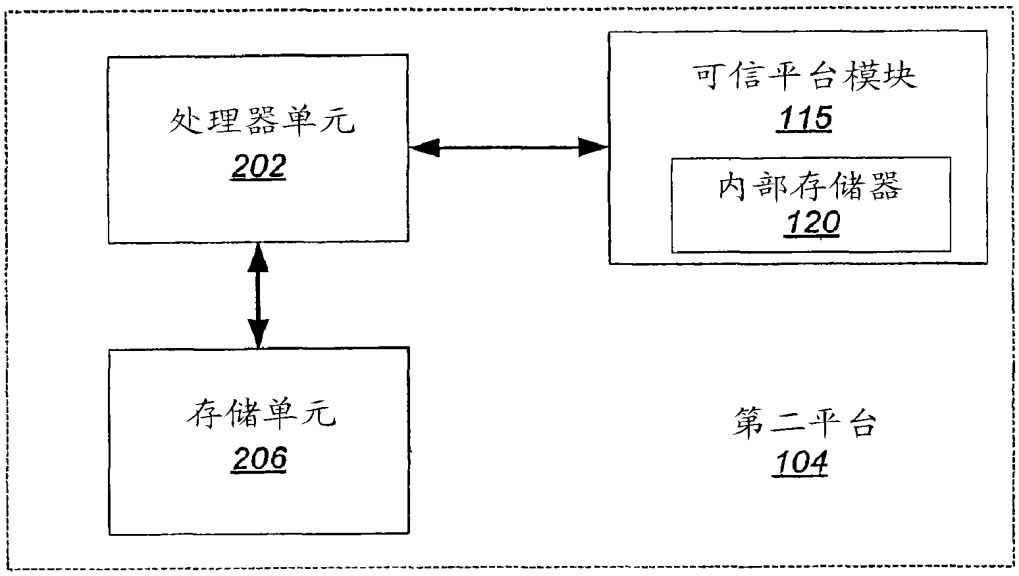

处理器单元
202
可信平台模块
115
内部存储器
120
存储单元
206
第二平台
104

图 3

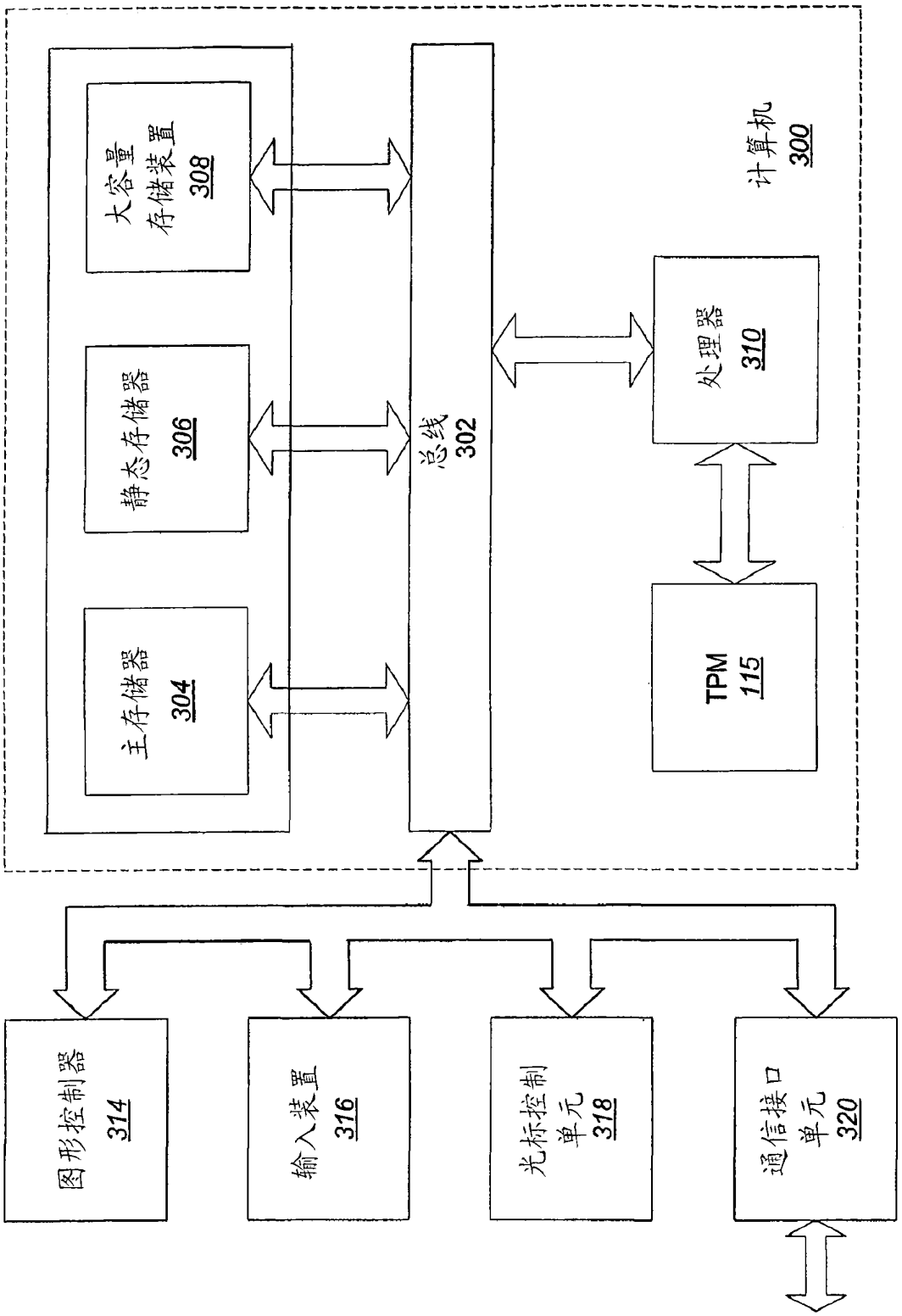

计算机
300
大容量
存储装置
308
静态存储器
306
主存储器
304
总线
302
处理器
310
TPM
115
104
图形控制器
314
输入装置
316
光标控制
单元
318
通信接口
单元
320

图 4

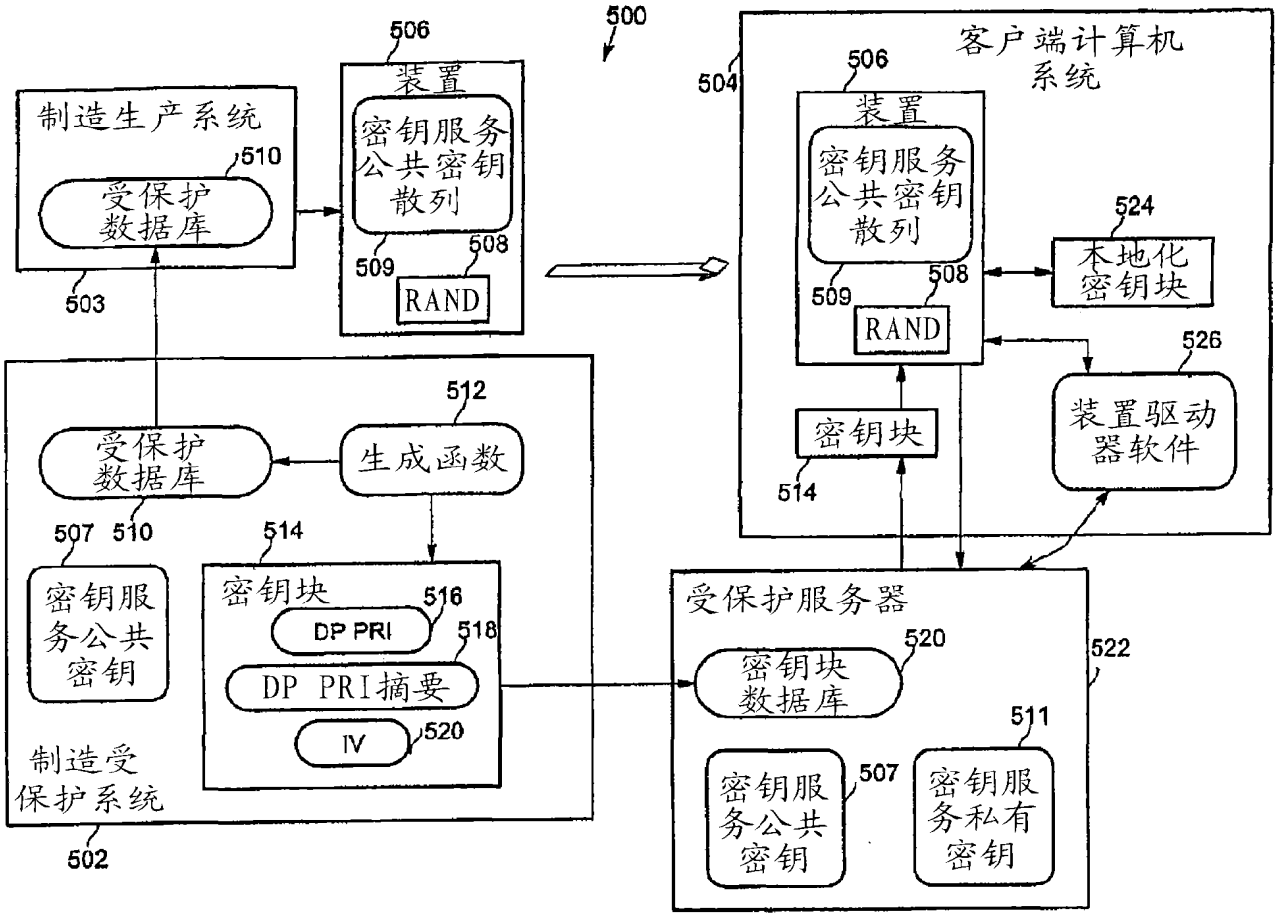

500
506
装置
密钥服务公共密钥散列
509
508
RAND
制造生产系统
510
受保护数据库
503
客户端计算机系统
504
506
装置
密钥服务公共密钥散列
509
508
RAND
524
本地化密钥块
526
装置驱动器软件
密钥块
514
512
生成函数
受保护数据库
507
510
密钥服务公共密钥
514
密钥块
516
DP PRI
518
DP PRI摘要
IV
520
制造受保护系统
502
受保护服务器
520
密钥块数据库
522
511
密钥服务公共密钥
507
密钥服务私有密钥

图 5

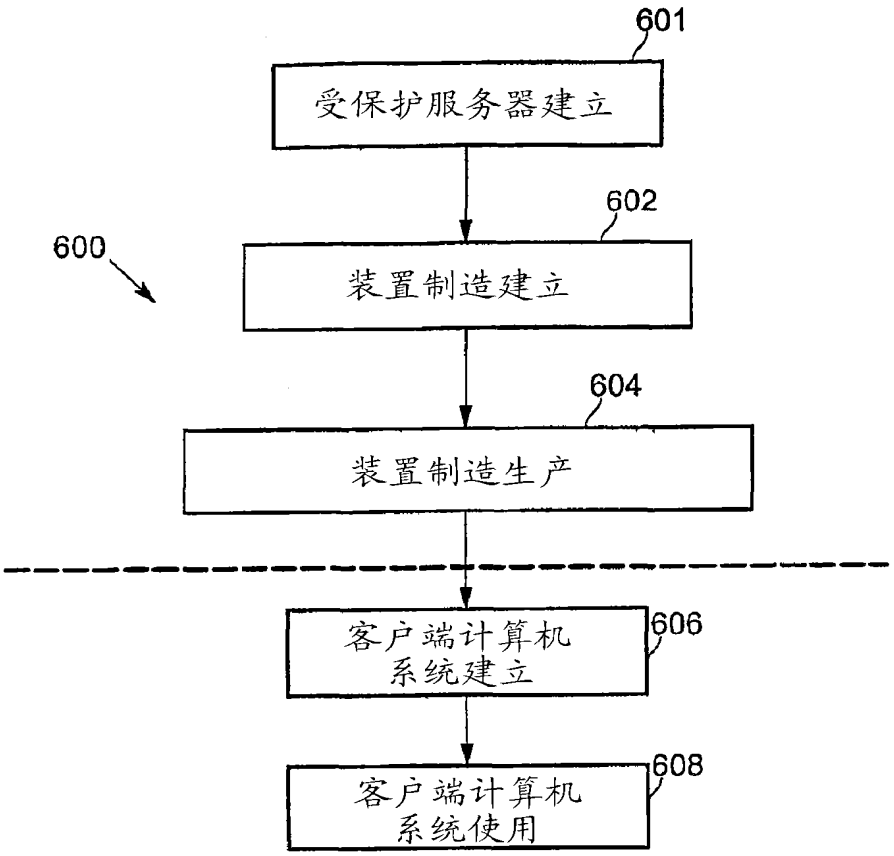

601
受保护服务器建立
602
600
装置制造建立
604
装置制造生产
客户端计算机
系统建立
606
客户端计算机
系统使用
608

图 6

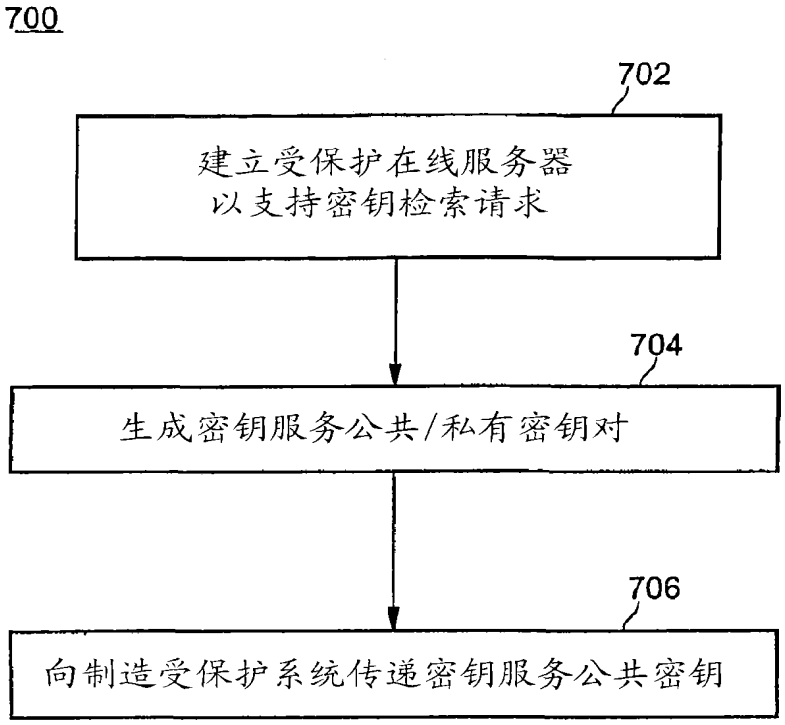

700
702
建立受保护在线服务器
以支持密钥检索请求
704
生成密钥服务公共/私有密钥对
706
向制造受保护系统传递密钥服务公共密钥

图 7

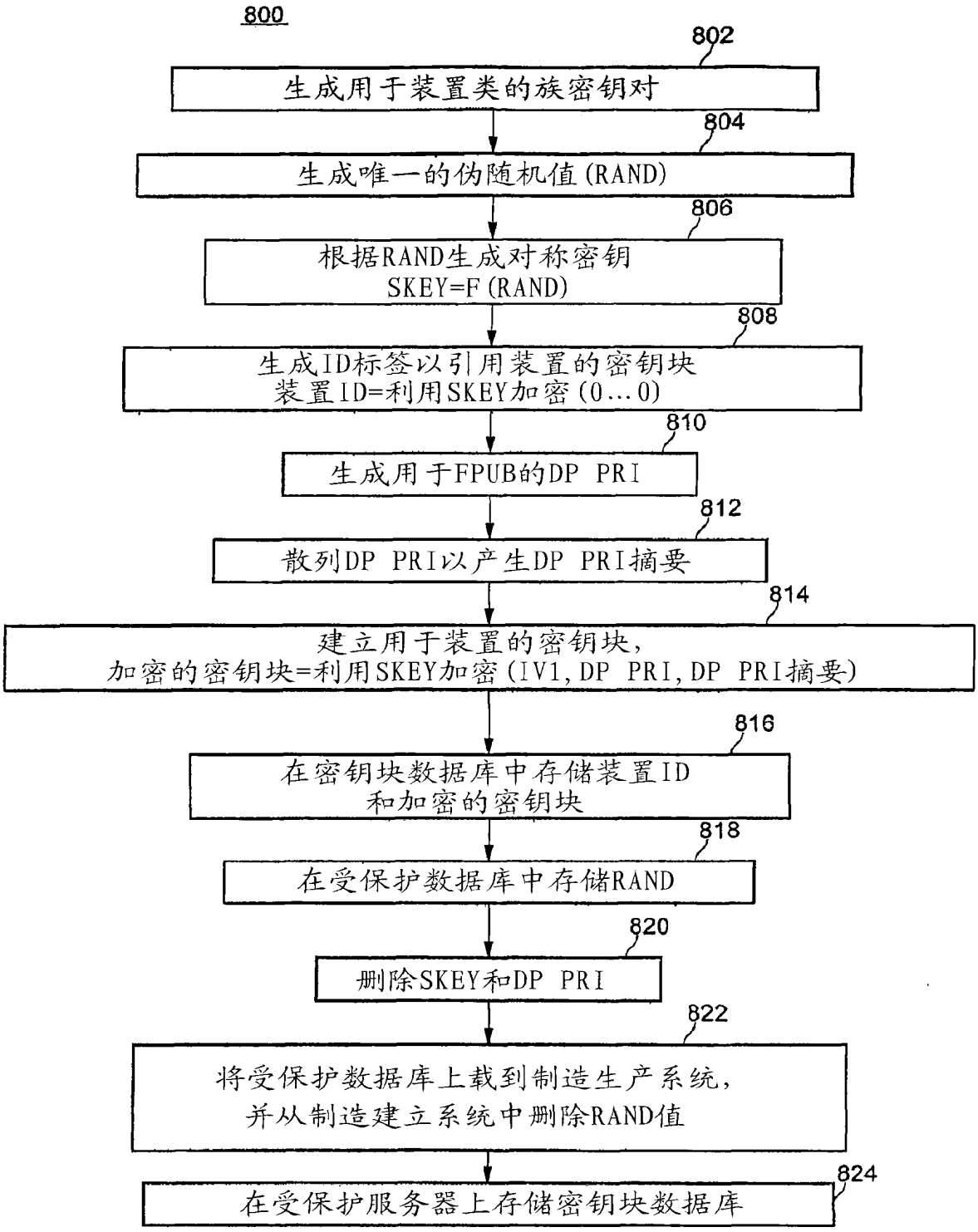

800
802
生成用于装置类的族密钥对
804
生成唯一的伪随机值(RAND)
806
根据RAND生成对称密钥
SKEY=F(RAND)
808
生成ID标签以引用装置的密钥块
装置ID=利用SKEY加密(0...0)
810
生成用于FPUB的DP PRI
812
散列DP PRI以产生DP PRI摘要
814
建立用于装置的密钥块,
加密的密钥块=利用SKEY加密(IV1,DP PRI,DP PRI摘要)
816
在密钥块数据库中存储装置ID
和加密的密钥块
818
在受保护数据库中存储RAND
820
删除SKEY和DP PRI
822
将受保护数据库上载到制造生产系统,
并从制造建立系统中删除RAND值
824
在受保护服务器上存储密钥块数据库

图 8

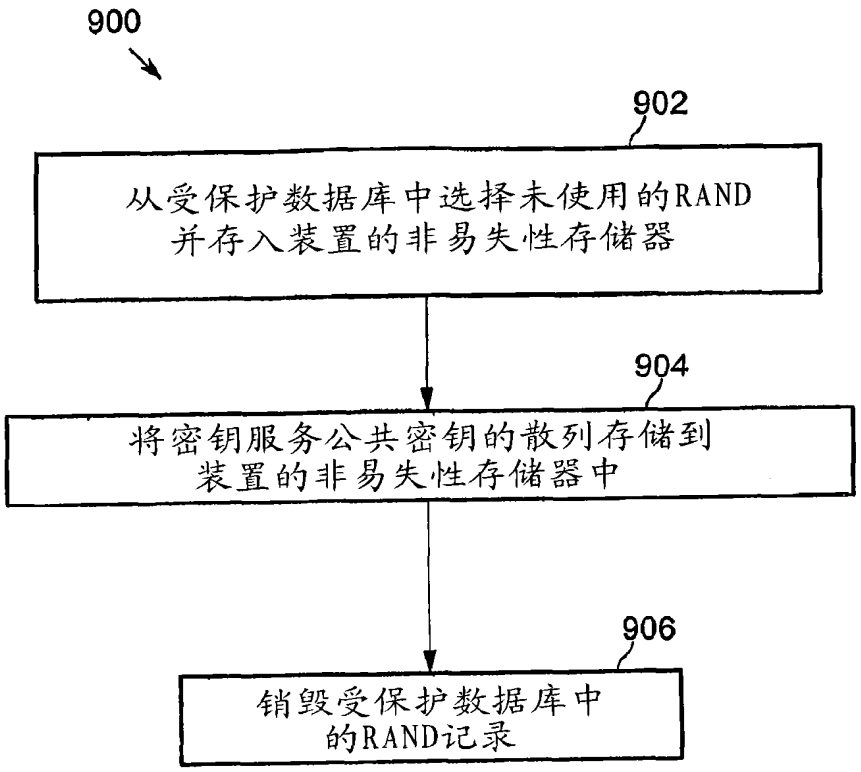

900
902
从受保护数据库中选择未使用的RAND
并存入装置的非易失性存储器
904
将密钥服务公共密钥的散列存储到
装置的非易失性存储器中
906
销毁受保护数据库中
的RAND记录

图 9

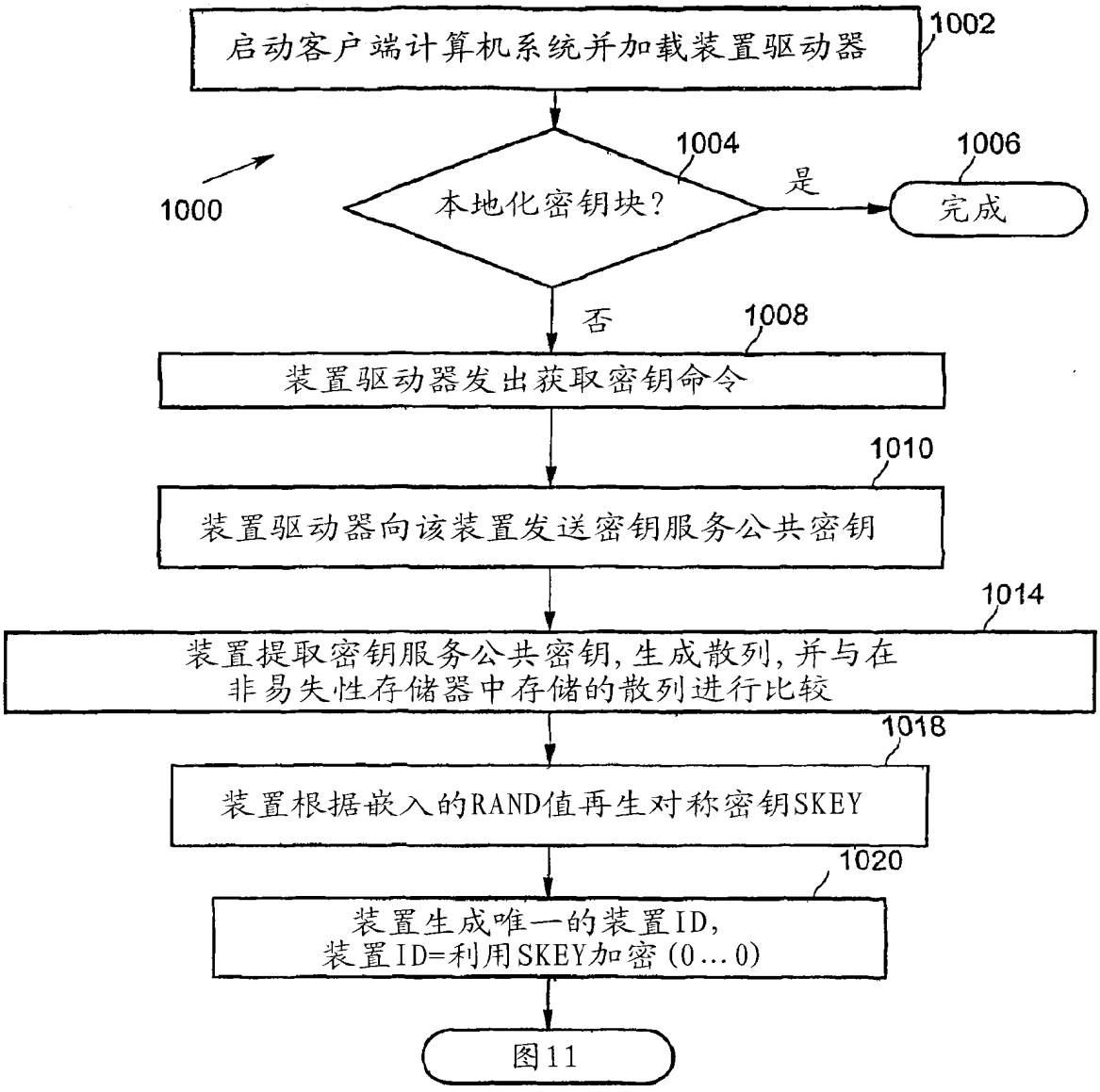

启动客户端计算机系统并加载装置驱动器
1002
1000
本地化密钥块?
1004
是
1006
完成
否
1008
装置驱动器发出获取密钥命令
1010
装置驱动器向该装置发送密钥服务公共密钥
1014
装置提取密钥服务公共密钥,生成散列,并与在非易失性存储器中存储的散列进行比较
1018
装置根据嵌入的RAND值再生对称密钥SKEY
1020
装置生成唯一的装置ID,
装置ID=利用SKEY加密(0...0)
图11

图 10

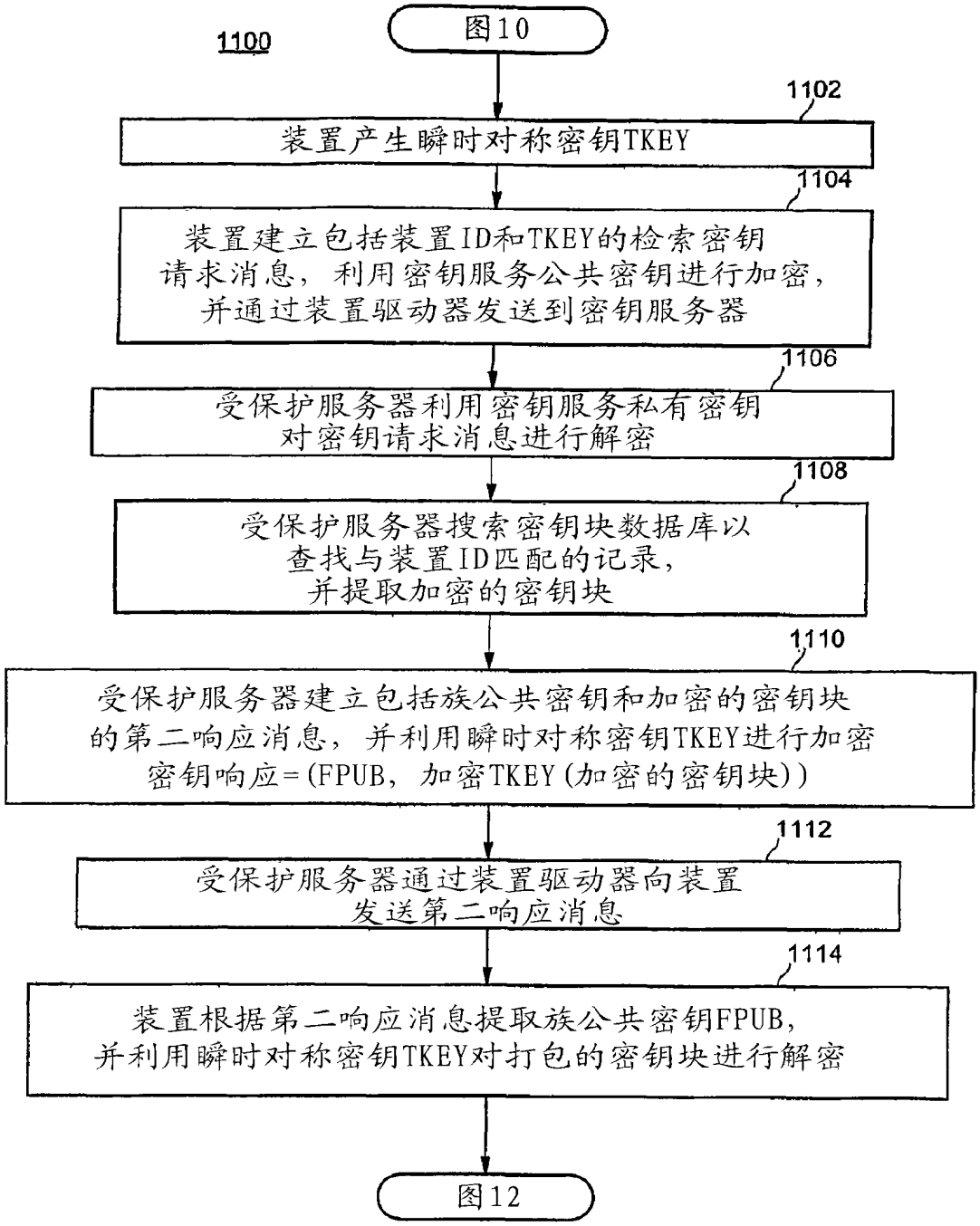

1100
图10
1102
装置产生瞬时对称密钥TKEY
1104
装置建立包括装置ID和TKEY的检索密钥
请求消息，利用密钥服务公共密钥进行加密，
并通过装置驱动器发送到密钥服务器
1106
受保护服务器利用密钥服务私有密钥
对密钥请求消息进行解密
1108
受保护服务器搜索密钥块数据库以
查找与装置ID匹配的记录，
并提取加密的密钥块
1110
受保护服务器建立包括族公共密钥和加密的密钥块
的第二响应消息，并利用瞬时对称密钥TKEY进行加密
密钥响应=(FPUB，加密TKEY(加密的密钥块))
1112
受保护服务器通过装置驱动器向装置
发送第二响应消息
1114
装置根据第二响应消息提取族公共密钥FPUB，
并利用瞬时对称密钥TKEY对打包的密钥块进行解密
图12

图 11

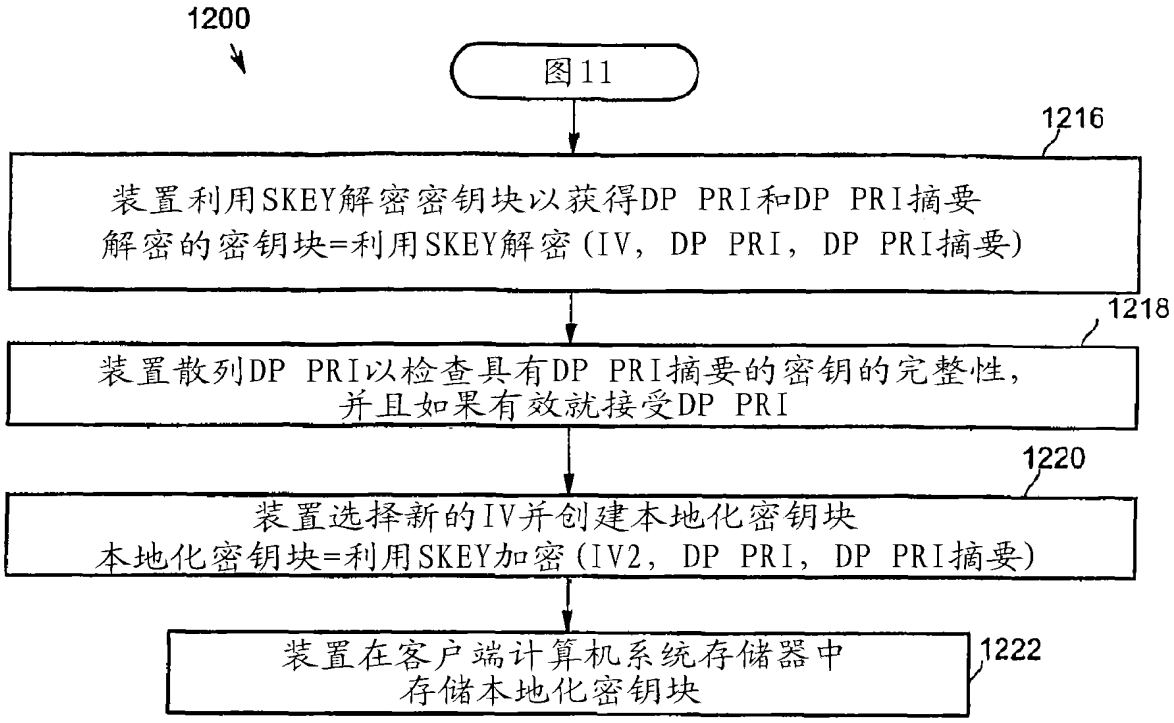

1200
图11
1216
装置利用SKEY解密密钥块以获得DP PRI和DP PRI摘要
解密的密钥块=利用SKEY解密(IV, DP PRI, DP PRI摘要)
1218
装置散列DP PRI以检查具有DP PRI摘要的密钥的完整性,
并且如果有效就接受DP PRI
1220
装置选择新的IV并创建本地化密钥块
本地化密钥块=利用SKEY加密(IV2, DP PRI, DP PRI摘要)
装置在客户端计算机系统存储器中
存储本地化密钥块
1222

图 12

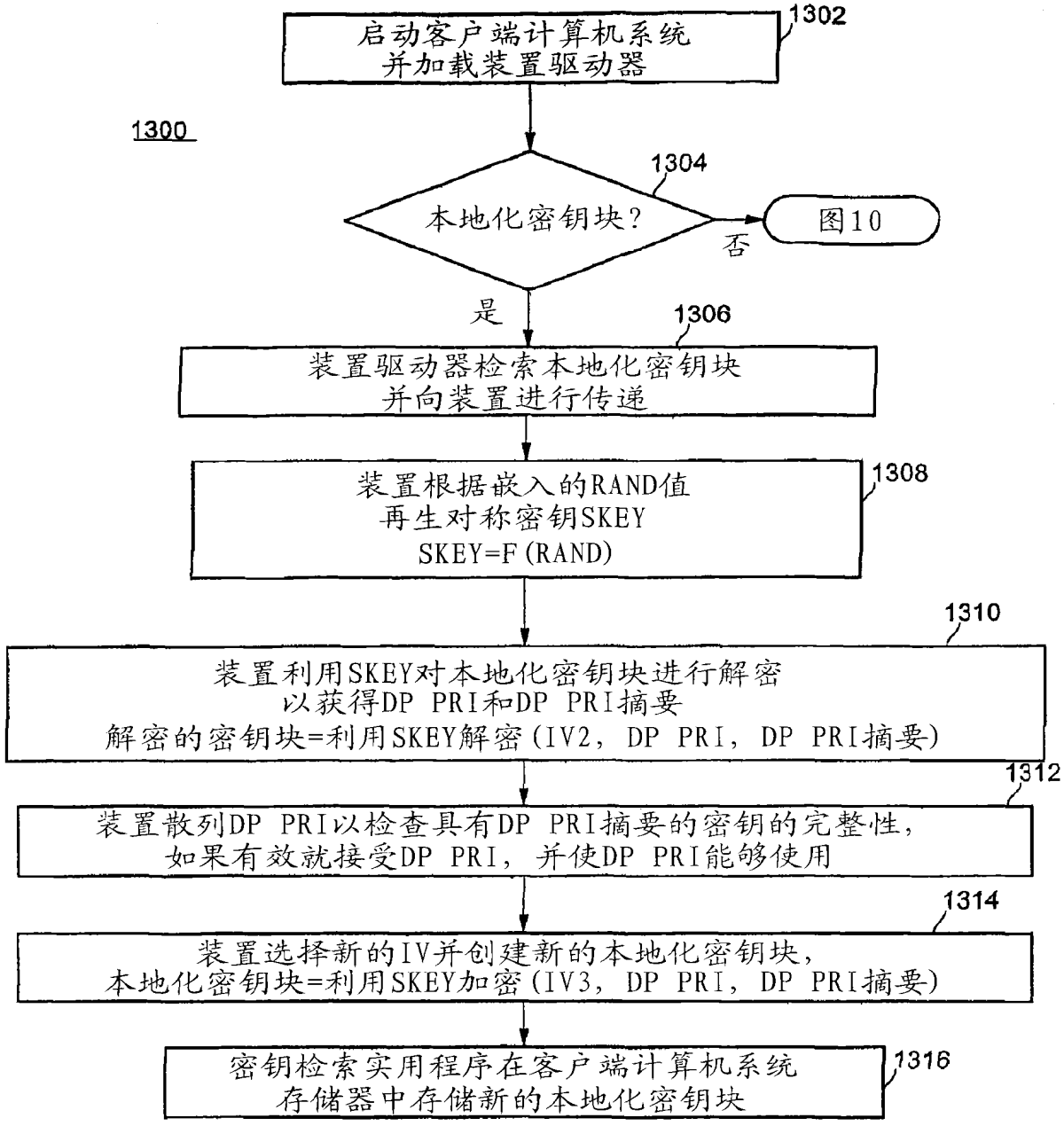

1300
启动客户端计算机系统
并加载装置驱动器
1302
本地化密钥块?
1304
图10
否
是
装置驱动器检索本地化密钥块
并向装置进行传递
1306
装置根据嵌入的RAND值
再生对称密钥SKEY
SKEY=F(RAND)
1308
装置利用SKEY对本地化密钥块进行解密
以获得DP PRI和DP PRI摘要
解密的密钥块=利用SKEY解密(IV2, DP PRI, DP PRI摘要)
1310
装置散列DP PRI以检查具有DP PRI摘要的密钥的完整性,
如果有效就接受DP PRI, 并使DP PRI能够使用
1312
装置选择新的IV并创建新的本地化密钥块,
本地化密钥块=利用SKEY加密(IV3, DP PRI, DP PRI摘要)
1314
密钥检索实用程序在客户端计算机系统
存储器中存储新的本地化密钥块
1316

图 13